BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT WORLD INTELLECTUAL PROPERTY International Bureau

WO 9608794A1

INTERNATIONAL APPLICATION PUBLISHED UNDER T

(51) International Patent Classification 6 : G07C 9/00 — A1

(11) International Publication Number: WO 96/08794

(43) International Publication Date: 21 March 1996 (21.03.96)

(21) International Application Number: PCT/US95/08792

(22) International Filing Date: 17 July 1995 (17.07.95)

(30) Priority Data: 08/304,346 12 September 1994 (12.09.94) US

(71) Applicant: WESTINGHOUSE ELECTRIC CORPORATION [US/US]; Westinghouse Building, Gateway Center, Pittsburgh, PA 15222 (US).

(72) Inventor: LEUNG, Edward, C.; 10383 Tonita Way, Cupertino, CA 95014 (US).

(74) Agents: SCHRON, Dean et al.; Westinghouse Electric Corporation, Law Dept., 11 Stanwix Street, Pittsburgh, PA 15222 (US).

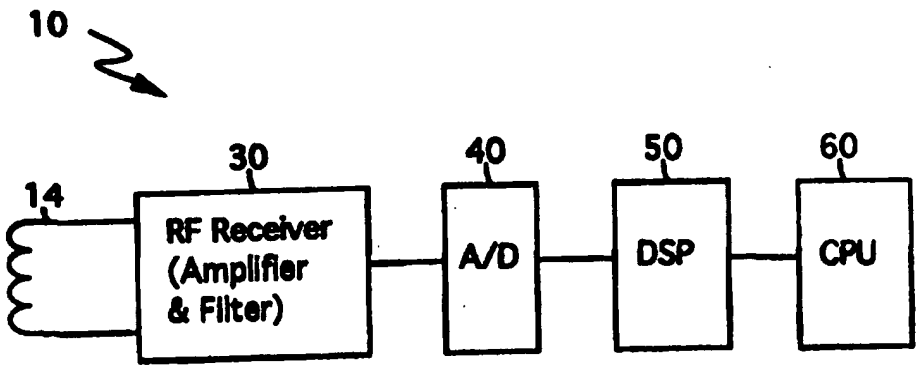
(81) Designated States: JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: SECURITY CODE IDENTIFICATION CIRCUIT

(57) Abstract

An access card reader includes a receive antenna (14) sensitive to a first signal generated by an access card. A receiver circuit (30) is coupled to the receive antenna to detect an analog second signal in the receive antenna. When the receive antenna is excited, the receiver conditions the analog second signal, and an analog to digital converter (40) converts the second signal into a digital security code. A processor (50) then determines the validity of the security code. In one aspect of the invention, the security code includes a plurality of fields including an 8-bit preamble field, a data field and an error detection field.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

SECURITY CODE IDENTIFICATION CIRCUIT

Field of the Invention

The present invention relates to a security code identification circuit.

Background of the Invention

Security systems are important for controlling personnel access to specific locations. Many modern security systems place a card reader at a secure entrance to read an access card. A person seeking access to a location positions the card in close proximity to the card reader which reads the card and then grants access to the location, if appropriate.

The card transmits a security code that is read by the reader. This security code typically has an identification field that the reader must identify and decode prior to granting access to the location.

A known approach uses a security code having two fields that include a preamble and a body. The preamble typically consists of 8 bits and the body of 32. However, these card readers suffer from two problems. The first is that analog reader components are sensitive to signal fluctuations and the positioning of the access card. The second is the inability to fully discern the preamble and the body due to their mode of analog operation. That is, because the circuit employs analog devices and is very sensitive to card position, the reader does not adequately characterize and store the full transmission and it does not verify the entire security code. The card reader uses only 3 of the 8 preamble bits in order to permit or deny

access to the location. This defeats the purpose of the 8 bit preamble and the 32 bits of data since the verification bit length is in direct proportion to the level of security and the difficulty that an unauthorized person would have in breaking the code to gain access. For instance, 3 bits provide only 8 possible combinations while 8 bits provide 256 possible combinations -- a much more secure code length.

An approach is needed that can discern the security code regardless of card position and that fully interprets and evaluates the security access code to provide tamper-resistant access to the secure location.

Summary of the Invention

The present invention describes an apparatus for receiving and verifying the whole security code preamble to improve the quality and reliability of security systems.

An access card reader includes a receive antenna sensitive to a first signal generated by an access card. A receiver circuit is coupled to the receive antenna to detect an analog second signal in the receive antenna. When the receive antenna is excited, the receiver conditions the analog second signal, and an analog to digital converter converts the second signal into a digital security code. A processor then determines the validity of the security code. In one aspect of the invention, the security code includes a plurality of fields including an 8-bit preamble field, a data field and an error detection field.

Several advantages arise from the invention including solid state identification of the security code, which improves the probability of proper verification. Another advantage is that the full security code preamble is verified, which improves security. Another advantage is that the quality and reliability of the product is increased.

Brief Description of the Figures

With reference to the accompanying figures:

Figure 1 is a schematic diagram of an access card and an access card reader;

Figure 2 is a graph illustrating bipolar phase shift keyed (BPSK) signal between the access card and the access card reader;

Figure 3 depicts a type of security code word information;

Figure 4 is a schematic diagram of the access card reader of Figure 1;

Figure 5 is a flowchart showing the card reader functions;

Figure 6 depicts a second type of security code word information;

Figure 7 is a graph illustrating quadrature phase shift keyed (QPSK) signal between the access card and the access card reader; and

Figure 8 depicts a network version employing the present invention.

Detailed Description of a Preferred Embodiment

The following description is provided to satisfy the patent statutes. Those skilled in the art will appreciate that various changes and modifications can be made while remaining within the scope of the present invention.

Figure 1 depicts a first embodiment of the invention showing an access card 20 and an access card reader 10. In the access card reader 10, an oscillator generates a 140 KHz signal that is communicated to transmit antenna 12. This signal has enough energy to cause an electro-magnetic field to form in the vicinity of the transmit antenna 12.

The access card 20, when it is placed within the vicinity of the card reader 10, receives energy on its receive antenna 22. This energy is accumulated and stored in the card 20, for example, by a diode and capacitor rectifier. The card 20 also uses the 140 KHz oscillating field to clock its circuitry at 70 KHz. Once sufficient energy is stored in the card 20, the card transmitter is activated and an RF security signal is transmitted from the card via transmit antenna 24 at 70 KHz using phase shift

keyed (PSK) modulation. The RF security signal is then received by the reader via receive antenna 14.

Receive antenna 14 is coupled to a receiver that conditions the analog security signal, e.g., amplifies and filters the analog security signal. To convert the signal from RF, the receiver demodulates the signal according to the type of modulation with which the signal was originally encoded. For example, Figure 2 is a graph illustrating a bipolar phase shift keyed (BPSK) signal transmitted by the access card 20 and received by the access card reader 10. This general type of phase shift keyed communication is known in the art and involves the receiver synchronizing up with the carrier and then looking for phase changes that represent data. In BPSK, there are two states that are represented as "0" and "1." Each of these states is correlated to a phase of the signal. For example, in-phase represents "0," and 180° out-of-phase represents "1." In this manner, the access card 20 transfers the identifying information to the access card reader 10. The access card reader 10 then verifies the security code to grant access to the location, if appropriate.

Using the code word of Figure 3, the card reader 10 synchronizes on the first bit transmitted. Then, the card reader interprets the succeeding 7 bits in the preamble and verifies the 8-bit preamble field. Thereafter, the card reader 10 receives the 32 bits of data and verifies the 32-bit data field.

As described with respect to Figure 1, the security code is received and verified by the access card reader 10. The elements depicted in Figure 4 are those that perform this function. The receive antenna 14 is connected to a receiver 30 that detects a current signal in the receive antenna 14. When current is excited in the receive antenna 14, the receiver 30 amplifies the current signal and filters the current signal by isolating the relevant frequency band of interest that is received from the access card 20. An analog to digital (A/D) converter 40 converts the analog current signal into a digital

form -- a digital security code. This converted digital security code is then delivered to a digital signal processor (DSP) 50 to verify the security code. The DSP 50, which has a memory associated therewith, performs a series of functions to verify the preamble and data that constitute the security code word before communicating it to a central processor unit 60.

Figure 5 is a flowchart 70 showing the card reader functions, which are primarily executed by the DSP 50. At the initialization step 72, the card reader has power and is broadcasting energy through transmit antenna 12 to maintain an electromagnetic field in the proximity of the card reader 10. Once an access card enters the area and is powered up, it transmits a signal that is received on receive antenna 14. The RF amplifier and filter 30 detects energy on the receive antenna 14 amplifies and filters the signal, and the A/D 40 converts the analog signal to digital data. In step 74, the DSP 50 receives the data and determines if sufficient energy is present in the signal to read the preamble.

When sufficient energy is present, the DSP 50 begins an integration function that accumulates the data in step 76. Then, in step 78, the DSP 50 performs a threshold comparison between the received data and a predetermined set threshold. If the received data is above the predetermined threshold, step 80 is performed.

Step 80 involves detecting the phase of the data signal. The DSP 50 takes the digital samples and sets the initial phase to 0°. This initial setting permits the DSP to compare subsequent phases against a known initial phase. As additional data is received, the DSP 50 compares the phase of the signal to the initial 0° phase and assigns data values to the phases where in-phase is a "0" and out-of-phase is a "1."

A sliding cross-correlation is performed between the received data and a valid preamble in step 82. This permits the DSP 50 to verify the preamble by comparing the received data against a valid preamble. If the preamble is

verified, step 84 is performed which informs the CPU 60 of the verification. Then the data from the succeeding fields -- if any -- is interpreted and recorded in step 86. Once the verification is complete, the security system permits the user to enter the location by, for example, unlocking the door. This system can also monitor the comings and goings of persons at a guarded gate by recording their personalized data encoded on their access card in the security code word.

The procedure outlined above has advantages over those previously developed. For one, the signal to noise ratio can be low since the digital signal processor is comparing the received code against a known valid code. That is, a cross-correlation between a received code and a known code permits a low signal to noise ratio signal to be properly interpreted. As a result, the access card reader 10 can properly interpret the access card 20 in a variety of positions that prior techniques may not have properly interpreted.

Another advantage is that because the DSP 50 has a memory associated therewith, the DSP can retain the incoming security code as well as a valid code to verify the entire preamble and can correlate the entire received signal against a valid security code.

The following is an example of an operational configuration. The access card reader generates a field signal at 140 KHz on the card reader transmit antenna. The access card generates a transmission signal with a 70 KHz carrier that is received by the card reader. The bit data rate is 8750 Hz so that each bit contains 8 carrier cycles. The data is phase encoded at 0° for a "0" and 180° for a "1." The A/D converter digitizes the received signal at a rate of 280K samples per second with 8 bits or resolution. The DSP, such as the Analog Devices ADSP2115, running at 64 MHz obtains the in-phase and out-of-phase values of the digitized signal. The DSP also performs integration of the digitized data and determines if the signal energy is above a predetermined threshold. The DSP decodes the preamble

data and, when there is a valid preamble match, the DSP verifies the preamble transmission and instructs the A/D converter to send the tag data, which the DSP then decodes.

Figure 6 depicts a second type of security code word information. This code word includes a plurality of fields for a security code word that identify a particular characteristic of the card. A mode field incorporates various operational parameters of the system, and parity and checksum fields incorporate error detection and correction. In the present invention, any field can be incorporated into the code word so long as the card has sufficient energy to transmit the data.

Figure 6 shows a blank field of 32 bits. In one aspect of the present invention, this field is intended to provide a no-transmit period of time in which the DSP 50 can verify the preamble before recording the data -- actually make the decision on the fly whether to record the data. This field can also be used, in another aspect of the invention, to permit the card to recharge in order to extend the security code word length. That is, if a card needs extra energy to transmit a long code word, a predetermined no-transmit period can permit the card to recharge before retransmitting the remainder of the code word.

Figure 7 is a graph illustrating quadrature phase shift keyed (QPSK) signal between the access card and the access card reader. In this type of transmission, four different phases represent four different data nibbles. For example, 0° represents "00," 90° represents "01," 180° represents "10," and 270° represents "11." This illustration shows that any type of keyed communication technique can be used with the present invention. Moreover, other communication techniques known in the art can be used in the present invention such as FSK, PMSK, FM and AM.

Figure 8 depicts a network version 90 employing the present invention. This configuration demonstrates how the invention might be deployed in a building or at a site. A plurality of card readers 92, 94, 96 are placed at

various locations around the site, such as at the doors or security stations. When a person seeks entrance to the site, he places his access card near one of the card readers and the card reader opens the door, if appropriate. At the same time, the central computer 98 can verify that the person is authorized to enter the location and log the entry location, date and time. The central computer 98 can also monitor a person's movements through various locations at the site and can log the person's entrance and exit from the site.

Having disclosed a preferred embodiment and the best mode, there are a number of modifications that will be obvious to one skilled in the art. This specification is intended to cover all embodiments within the spirit of the invention that is claimed.

CLAIMS:

1. In a security access circuit, the combination comprising:

a receive antenna sensitive to a first signal generated by an access card providing information associated with said card;

a receiver circuit coupled to said receive antenna to detect receipt of said first signal by said receive antenna and generate an analog second signal providing said information;

an analog to digital converter coupled to said receiver circuit to convert said analog second signal into a digital security code; and

a processor coupled to said analog to digital converter to receive said digital security code and to determine the validity of said security code.

2. The security access circuit of claim 1, wherein said first signal is a radio-frequency signal.

3. The security access circuit of claim 1, wherein said analog to digital converter converts said second signal into a digital security code that includes a plurality of fields.

4. The security access circuit of claim 1, wherein said analog to digital converter converts said second signal into a digital security code that includes an 8-bit preamble.

5. The security access circuit of claim 1, wherein said analog to digital converter converts said

second signal into a digital security code that includes an error detection field.

6. The security access circuit of claim 1, wherein:

said first signal includes phase shift keyed information.

7. The security access circuit of claim 1, further comprising:

a transmit antenna to generate a third signal to power said access card.

8. The security access circuit of claim 7, wherein:

said access card receives said third signal from said transmit antenna and generates said first signal in response thereto.

9. A security access network comprising in combination:

a plurality of access card readers each having a receive antenna sensitive to a first signal generated by an access card, a receiver circuit coupled to said receive antenna to detect a second signal in said receive antenna and to amplify and filter said second signal to generate a third signal, an analog to digital converter coupled to said receiver circuit to convert said third signal to generate a digital security code, and a processor coupled to said analog to digital converter to receive said digital security code and to determine the validity of said security code; and

a central computer coupled to said plurality of access card readers to communicate with said access card readers and to log the use of said access card.

10. The network of claim 9, wherein:

said security code includes a plurality of fields.

11. A method of operating a security access circuit, comprising the steps of:

receiving a first signal from an access card that provides information associated with said card;

detecting receipt of said first signal and generating an analog second signal providing said information;

converting said analog second signal into a digital security code;

determining if said security code is valid; and

when said security code is valid, initiating a signal verifying said security code.

12. The method of claim 11, wherein:

said converting step involves converting said analog second signal into a digital security code that comprises a plurality of fields.

13. The method of claim 12, wherein:

one of said fields is an 8-bit preamble.

14. The security access circuit of claim 12, wherein:

one of said fields is an error detection field.

15. The method of claim 11, wherein:

said receiving step involves receiving said first signal that includes phase shift keyed information.

16. The method of claim 11, further comprising:

transmitting a third signal to stimulate said access card.

17. The method of claim 11, further comprising:

transmitting said security code to a central computer.

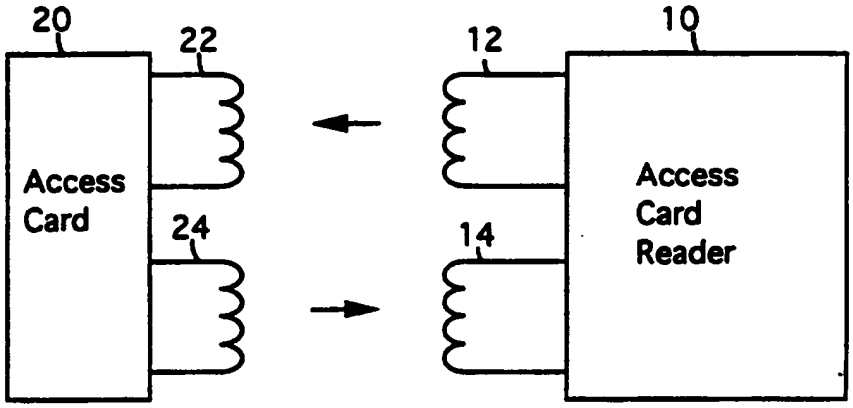


Figure 1

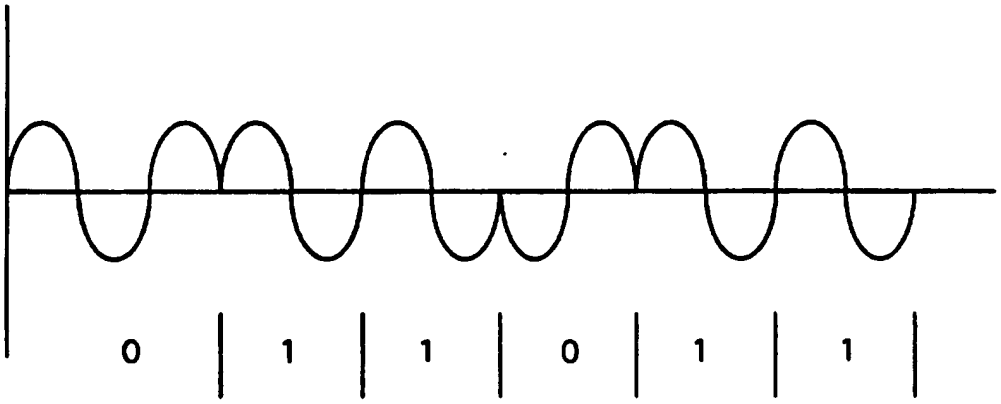


Figure 2

Figure 3

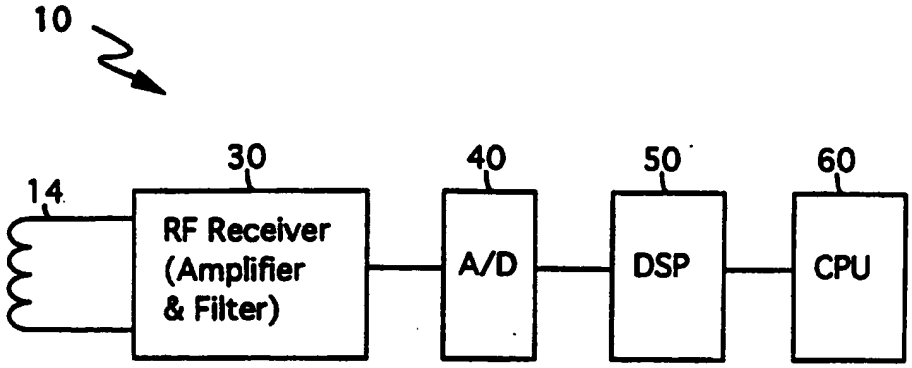


Figure 4

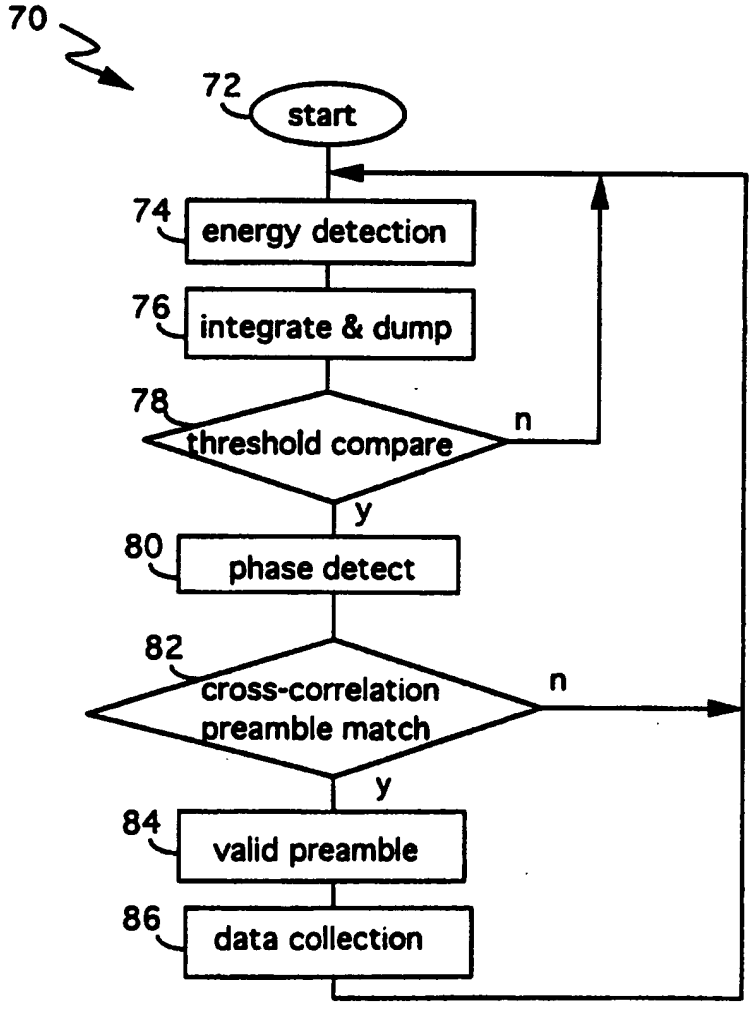


Figure 5

preamble	blank	tag	mode	parity	checksum
8	32	32	4	4	8

Figure 6

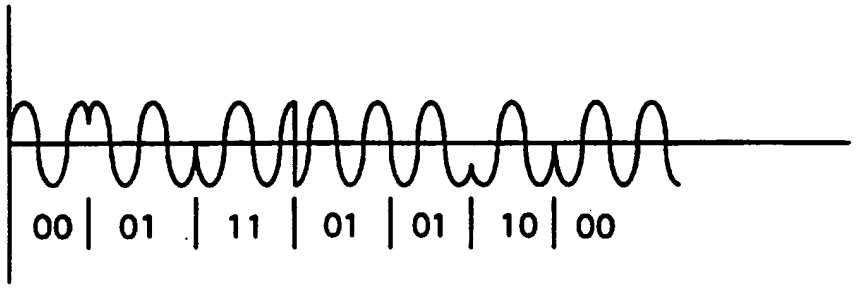


Figure 7

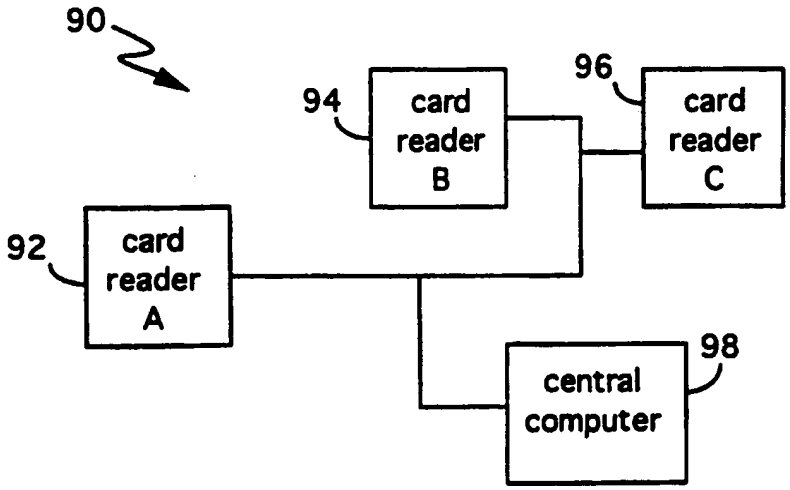


Figure 8

INTERNATIONAL SEARCH REPORT

Inte.. ..onal Application No
PCT/US 95/08792

A. CLASSIFICATION OF SUBJECT MATTER

G 07 C 9/00

According to International Patent Classification (IPC) or to both national classification and IPC 6

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G 07 C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, A, 91/06 926 (SECURITY DYNAMICS TECHNOLOGIES) 16 May 1991 (16.05.91), fig. 1; page 8, line 6 - page 10, line 10; page 13, lines 16-28.	11,12, 16
A	--	1,2,9
A	EP, A, 0 306 598 (CLIFFORD ELECTRONICS) 15 March 1989 (15.03.89), fig. 1; column 7, lines 18-30.	1,2,9, 11
A	-- DE, A, 3 305 685 (SENSORMATIC ELECTRONICS) 15 September 1983 (15.09.83), fig. 2,4,7; page 16,	1,2,9, 11

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 1995	11. 12. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	DRÖSCHER e.h.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna... al Application No
PCT/US 95/08792

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	lines 24-32; page 20, lines 3-14; claim 1. ----	

ANHANG

Internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX

to the International Search Report to the International Patent Application No.

ANNEXE

au rapport de recherche international relatif à la demande de brevet international n°

PCT/US 95/08792 SAE 114877

In diesem Anhang sind die Mitglieder der Patentfamilien der in obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présénte annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsibilité de l'Office.

In Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A1 9106926	16-05-91	US A 5097505	17-03-92
		AU A1 67208/90	31-05-91
		AU A1 79816/91	20-05-92
		AU B2 642362	14-10-93
		AU B2 649190	12-05-94
		CA AA 2072150	01-05-91
		CA AA 2094026	20-04-92
		EP A1 497889	12-08-92
		EP A1 555219	18-08-93
		JP T2 5503598	10-06-93
		JP T2 6507277	11-08-94
		WO A1 9207436	30-04-92
		US A 5058161	15-10-91
		US A 4720860	19-01-88
		US A 4856062	08-08-89
		US A 4885778	05-12-89
		US A 4998279	05-03-91
		US A 5023908	11-06-91
		US A 5168520	01-12-92
		US A 5367572	22-11-94
		AT E 71754	15-02-92
		AU A1 65686/86	04-06-87
		AU B2 587087	03-08-89
		DE C0 3683481	27-02-92
		EP A2 234100	02-09-87
		EP A3 234100	27-04-88
		EP B1 234100	15-01-92
		ES T3 2029450	16-08-92
		JP A2 63024384	01-02-88
EP A2 306598	15-03-89	EP A3 306598	23-08-89
		US A 5146215	08-09-92
		US A 4922234	01-05-90
		US A 5157375	20-10-92
		US A 4887064	12-12-89
DE A1 3305685	15-09-83	AR A1 231364	31-10-84
		BE A1 895864	30-05-83
		BR A 8301091	22-11-83
		CA A1 1211522	16-09-86
		DE C2 3305685	19-10-95
		ES A1 519769	16-08-84
		ES A5 519769	17-09-84
		ES A1 8407270	16-11-84
		FR A1 2522829	09-09-83
		FR B1 2522829	05-09-86
		GB A0 8305854	07-04-83
		GB A1 2116808	28-09-83
		GB B2 2116808	22-10-86
		IT A0 8309358	04-03-83
		IT A 1198536	21-12-88
		JP A2 58162881	27-09-83
		JP B4 3002271	14-01-91
		MX A 155097	26-01-88
		NL A 8300643	03-10-83
		SE A0 8301199	04-03-83
		SE A 8301199	06-09-83
		SE B 456278	19-09-88
		SE C 456278	19-01-89
		US A 4471345	11-09-84